Framework for Improving Critical Infrastructure Cybersecurity

June 2017

cyberframework@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Charter

Improving Critical Infrastructure Cybersecurity

February 12, 2013

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

Executive Order 13636

December 18, 2014

Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

"…on an ongoing basis, facilitate and support the development of a ***voluntary***, ***consensus-based***, ***industry-led*** *set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure"*

Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

Key Attributes

It's meant to be customized

It's a framework, not a prescriptive standard

- Provides a *common language* and systematic methodology for managing cyber risk.
- Does not tell an organization *how* much cyber risk is tolerable, nor provide "the one and only" formula for cybersecurity.
- Enable best practices to become *standard practices for everyone* via common lexicon to enable action across diverse stakeholders.

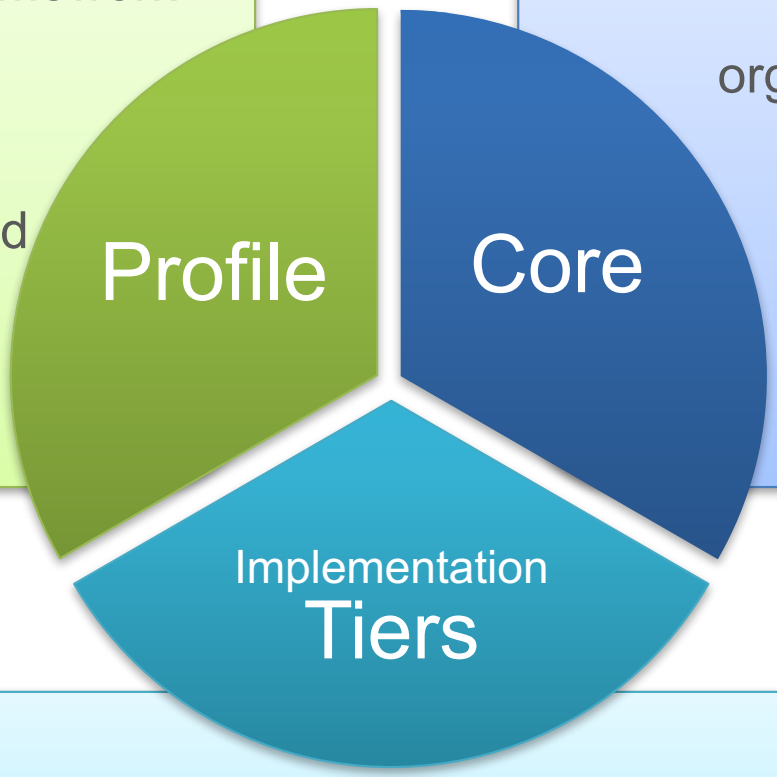
It's a living document

- Can be updated as stakeholders *learn from implementation*
- Can be updated as *technology and threats* changes.

Cybersecurity Framework Components

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Implementation Tiers

Cybersecurity Framework Component

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization benefits my sharing or receiving information from outside parties			

Core

Cybersecurity Framework Component

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
What safeguards are available?	Protect	Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

Core – Example

Cybersecurity Framework Component

Function	Category	Subcategory	Informative Reference
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1

Profile

Cybersecurity Framework Component

Ways to think about a Profile:

- A customization of the Core for a given sector, subsector, or organization.
- A fusion of business/mission logic and cybersecurity outcomes.
- An alignment of cybersecurity requirements with operational methodologies.
- A basis for assessment and expressing target state.
- A decision support tool for cybersecurity risk management.

Framework 7-Step Process

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implementation Action Plan

Work in Progress: Framework Roadmap

Authentication

Automated Indicator Sharing

Conformity Assessment

Cybersecurity Workforce

Data Analytics

Federal Agency Cybersecurity Alignment

International Aspects, Impacts, and Alignment

Supply Chain Risk Management

Technical Privacy Standards

Cybersecurity Executive Order

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Risk Management:

(ii) "…agency head **shall use** The Framework" and

"…provide a risk management report within 90 days containing a description of the "…agency's **action plan to implement the Framework**."

Proposed Federal Usage

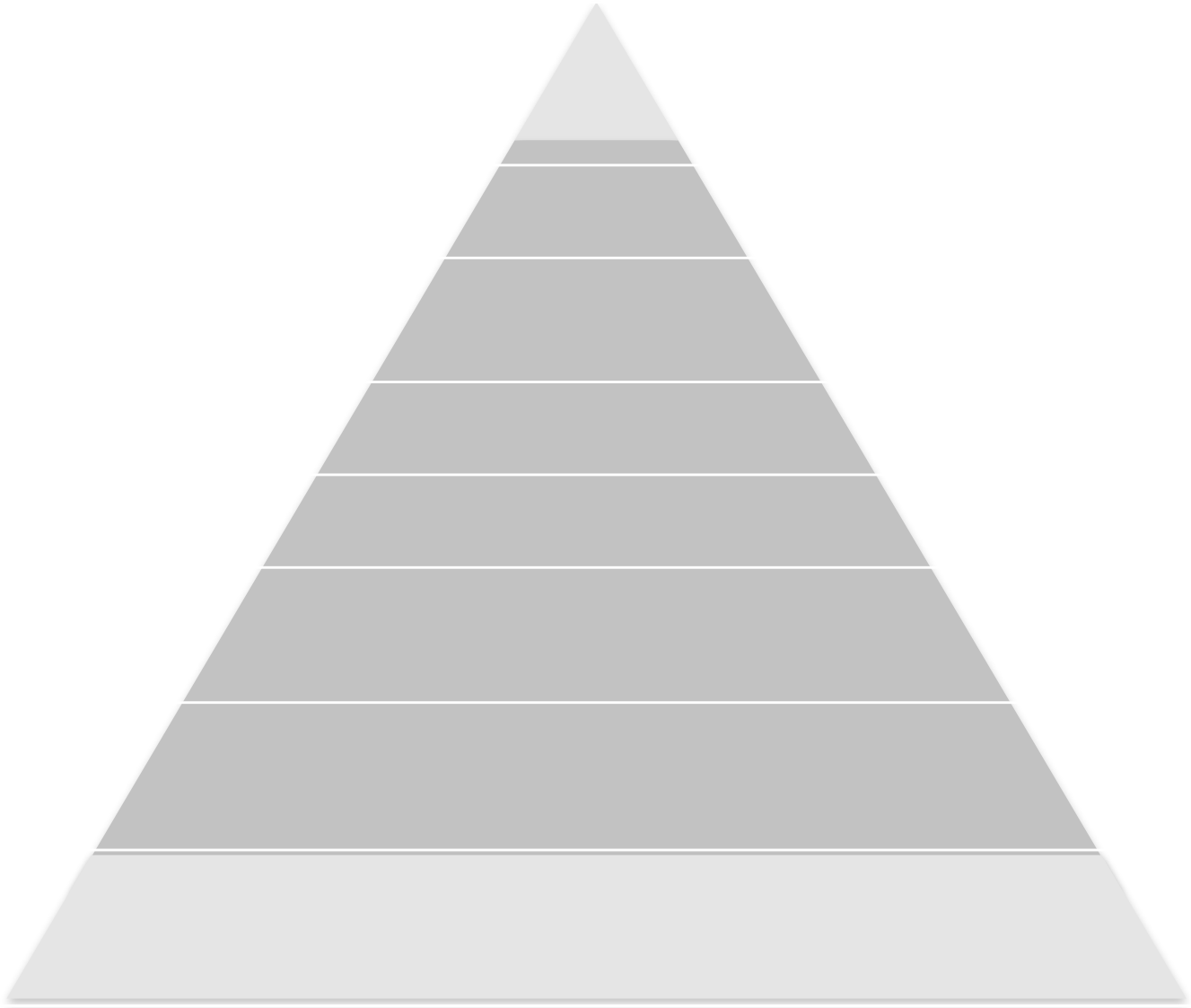
NIST IR 8170 The Cybersecurity Framework: Implementation Guidance for Federal Agencies

Special Publication 800-39

Level 1
Org

Level 2
Mission/ Business Processes

Level 3
System

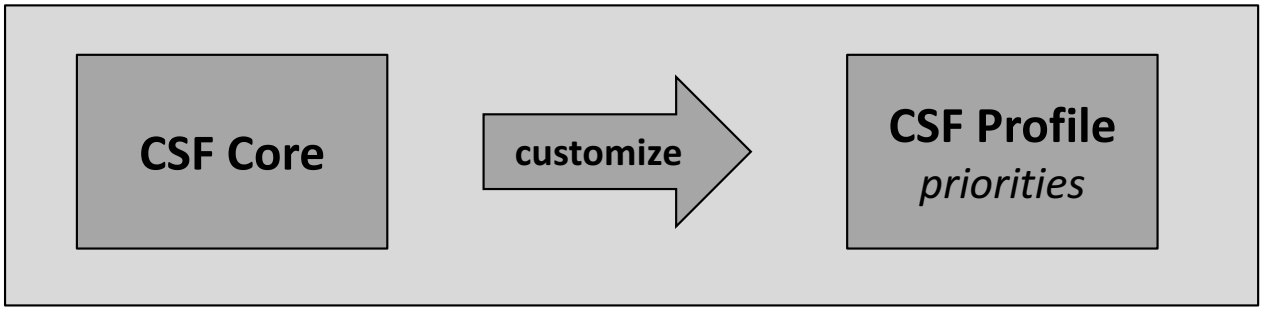


Proposed Federal Usage

NIST IR 8170 The Cybersecurity Framework: Implementation Guidance for Federal Agencies

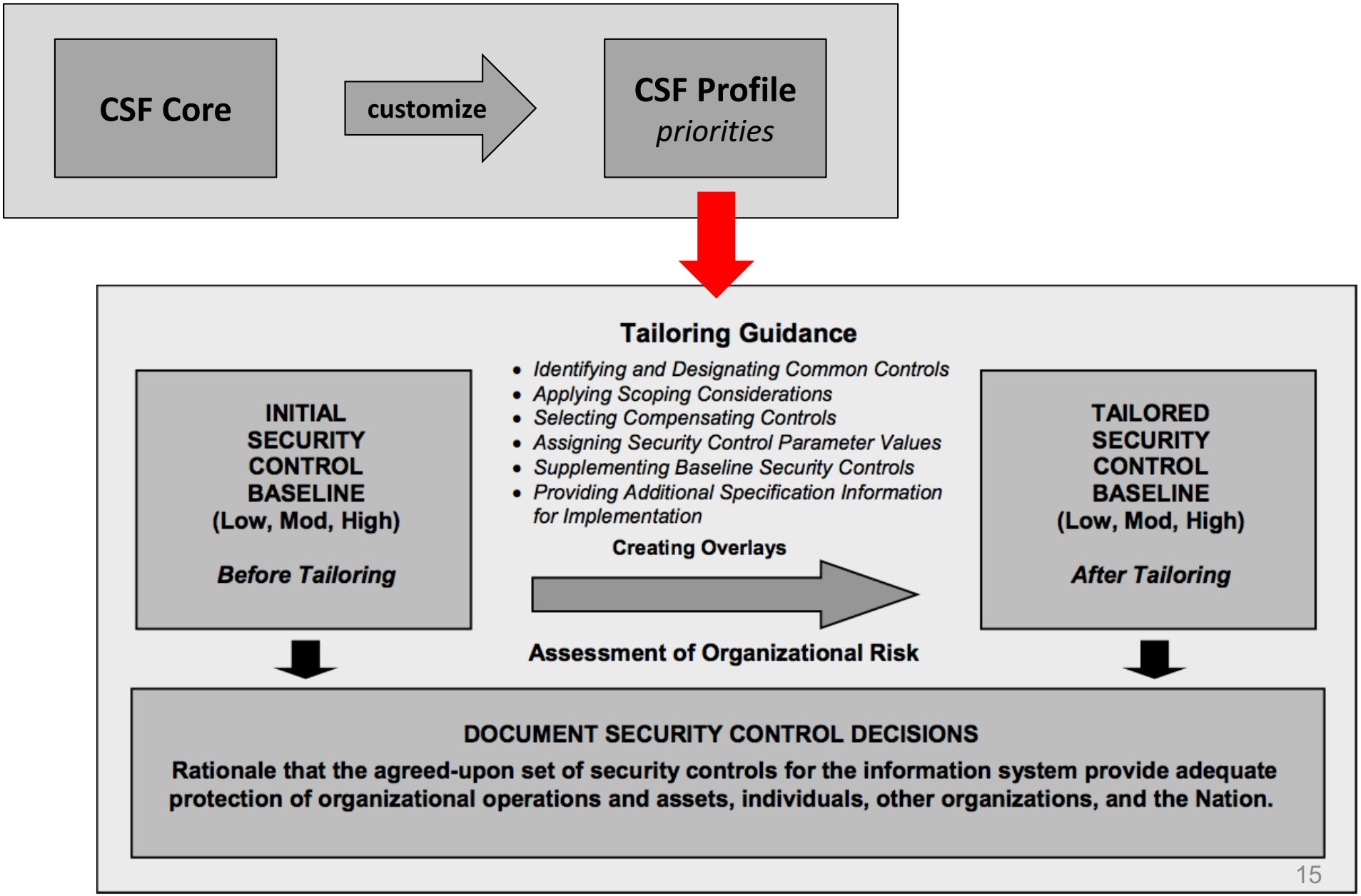
Inform the Tailoring Process

Example of Use 8 of 8



Inform the Tailoring Process

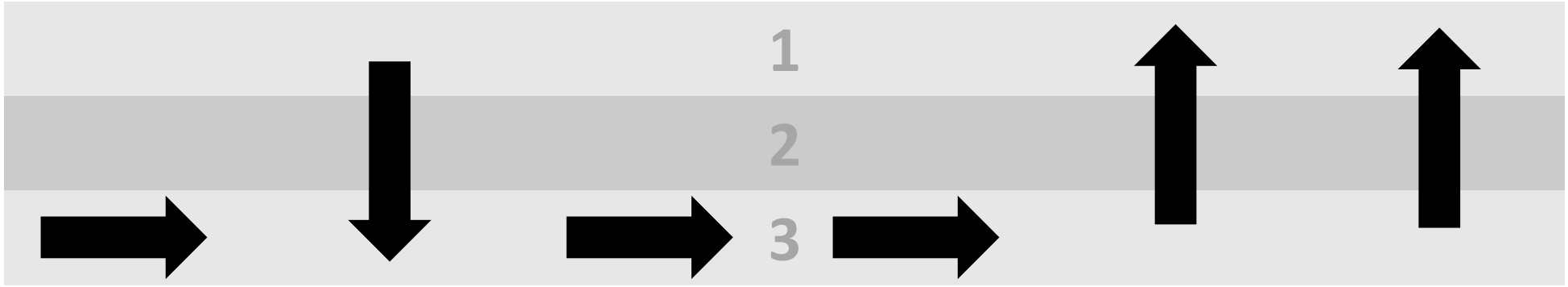
Example of Use 8 of 8



Predominant RMF Activity

Categorize	Select	Implement	Assess	Authorize	Monitor
Determine system mission/ business impact	Finalize controls baseline using stakeholder input	Deploy controls baseline	Determine, analyze, and document risk state	Consider risk state and make operating decision	Communicate risk status for continuous authorization

Predominant Tier Flow



Categorize	Select	Implement	Assess	Authorize	Monitor
Determine system mission/ business impact	Finalize controls baseline using stakeholder input	Deploy controls baseline	Determine, analyze, and document risk state	Consider risk state and make operating decision	Communicate risk status for continuous authorization

Cybersecurity Framework Helps When Spanning Tiers

Workflow & Translation

Detail/ Expand

Summarize/ Abstract

"Tier" SP 800-39	"Roles" SP 800-39	"Stakeholders" Cybersecurity Framework	"Core" Cybersecurity Framework
Level 1 *Organization*	…	Senior Executives	Identify, Protect, Detect, Respond, Recover *as "Functions"*
Level 2 *Mission/ Business Processes*	…	Business Process Personnel	22 Categories 98 Subcategories SP 800-53 controls *as "Informative References"*
Level 3 *System*	…	Implementation Personnel	

Resources

Where to Learn More and Stay Current

Framework for Improving Critical Infrastructure Cybersecurity and related news, information:

www.nist.gov/cyberframework

Additional cybersecurity resources:
http://csrc.nist.gov/

Questions, comments, ideas:
cyberframework@nist.gov